Penggunaan Algoritma SHA-256 Sebagai Pengganti Algoritma MD5 Pada IPSec

M WAHYU PUJIUTOMO
Program Studi Teknik Informatika - S1, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang
URL : http://dinus.ac.id/
Email : gambaz.poll@gmail.com

ABSTRAK

Keamanan pada komunikasi melalui jaringan komputer sekarang telah menjadi persoalan penting. Teknik kriptografi diimplementasikan pada protokol komunikasi IPSec untuk mendapatkan aspek keamanan tersebut. IPSec merupakan serangkaian protokol komunikasi yang menerapkan beberapa teknik kriptografi untuk menjamin keamanan dalam komunikasi melalui jaringan komputer.IPsec merupakan solusi yang transparan terhadap pengguna karena pengguna tidak perlu menyadari keberadaannya karena IPSec membungkus paket-paket IP dengan header yang pada akhirnya ditransmisikan sebagai paket-paket IP biasa. Protokol Authentification Header (AH) menjamin data integrity, sedangkan Encapsulating Security Payload (ESP) selain menjamin data integrity juga menjamin data confidentiality.Untuk menjamin data integrity, IPSec menggunakan HMAC (Hash Message Authentication Code) yang berupa algoritma yang mempunyai kunci yang rahasia. HMAC menggunakan fungsi hash satu arah. Algoritma SHA-256 dan MD5 adalah beberapa contoh algoritma yang dipakai pada IPSec.Tetapi saat ini telah ditemukan collision pada algoritma MD5, sehingga tidak lagi dianggap sebagai algoritma yang aman digunakan. Pada algoritma SHA-256 yang relatif masih baru, belum ditemukan collision yang menyebabkan 2 data yang berbeda tetapi menghasilkan 1 buah enkripsi yang sama.Algoritma SHA-256 bukanlah algoritma yang sempurna sebagai authentication code. Banyaknya waktu yang dibutuhkan untuk proses enkripsi yang sering menjadi kendala. Tetapi hingga kini SHA-256 masih dianggap sebagai algoritma yang masih sangat bagus untuk digunakan pada IPSec.

Kata Kunci : kriptografi, algoritma, SHA-256, MD5

Using SHA-256 Algorithm as Replacement of MD5 Algorithm in IPSec

M WAHYU PUJIUTOMO
Program Studi Teknik Informatika - S1, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang
URL : http://dinus.ac.id/
Email : gambaz.poll@gmail.com

ABSTRACT

Security in communication through computer networks has now become an important issue. Cryptographic techniques implemented on the IPSec communication protocol to obtain the security aspect. IPSec is a set of communications protocols that implement several cryptographic techniques to ensure the security of communications over computer networks.IPSec is a solution that transparent to the user because the user does not need to be aware of its existence because IPSec wrap IP packets with a header that eventually transmitted as normal IP packets. Authentication protocol Header (AH) to ensure data integrity, while the Encapsulating Security Payload (ESP) in addition to ensuring data integrity also ensures data confidentiality.To ensure data integrity, IPSec uses HMAC (Hash Message Authentication Code) in the form of algorithms that have the secret key. HMAC uses a one-way hash function. SHA-256 algorithm and MD5 are some examples of algorithms that used in IPSec.But today has found a collision in the MD5 algorithm, so it is no longer considered as a secure algorithm to use. SHA-256 algorithms are relatively new, not yet found a collision that led to two different data but generate the same encryption.Algorithm SHA-256 algorithm is not perfect as the authentication code. The amount of time that required for the encryption process is often a constraint. But until now SHA-256 algorithm which is still regarded as still very good for use in IPSec.

Keyword : kriptografi, algoritma, SHA-256, MD5